INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Fingerprint Voting System for Departmental Elections

[1]Prof. Disha Deotale, [2]Ayush Punvatkar, [3]Abhijit Wankhede, [4]Yogesh Bhoyar, [5]Balaji Jadhav, [6]Aishwarya Dangri

[1,2,3,4,5,6]Department Computer Science and Engineering, Shri Shankar Prasad Agnihotri College of Engineering Wardha, Wardha, Maharashtra, India

[1]dishadeotale27@gmail.com, [2]ayushpunvatkar3@gmail.com, [3]abhiwankhede661@gmail.com, [4]yogeshbhoyar2003@gmail.com, [5]balaji8177846001@gmail.com, [6]adangri1999@gmail.com

Article History

Received on: 10 Feb. 2025
Revised on: 28 Feb. 2025
Accepted on: 30 March 2025

Keywords: Voting, Fingerprint, Machine, Thumb etc.

e-ISSN: 2455-6491

DOI: 10.5281/zenodo.15400672

Production and hosted by.
www.garph.org

ABSTRACT

Intended to enhance security, accuracy, and openness, a fingerprint voting system for departmental elections is an electronic voting system based on biometrics. Using fingerprint verification to validate voters' identities, this method lowers the risk of unauthorised access, identity theft, and several votes. Validly kept in a database are fingerprints of voters amassed throughout registration. Before being permitted to vote on election day, voters confirm their identity by means of a fingerprint scanner. The system ensures that every voter is allowed to vote just once, hence discouraging election fraud. Digital recording of votes ensures data integrity and enables fast and accurate counting. Encryption methods preserve voter information and defend against online dangers. This mechanism lowers reliance on physical ballot papers, therefore is both cost-effective and environmentally friendly. Real-time vote counting also streamlines the election process and lessens the human involvement required. By guaranteeing equity, safety, and user-friendliness, a fingerprint-based voting system enhances the credibility and efficiency of departmental polls. It also helps to assure that the system is independent.

1. INTRODUCTION

Democratic decision-making processes depend much upon elections, which guarantee people legitimate right to select their representatives in an open and equitable way. Usually susceptible to problems like voter fraud, impersonation, dual voting, and delays in result processing are conventional voting methods like manual vote counting and paper ballots. Secure and effective alternatives provided by biometric-based voting systems—especially fingerprint verification—have arisen to deal with these problems. Using biometric technology, a fingerprint voting system checks voter identities before they can cast their votes so removing the possibility of unauthorized access and duplication.

Before the election, voters capture their fingerprints in a database stored securely in a fingerprint-based electoral system. They verify themselves with a fingerprint scanner on voting

day so that only qualified voters engage. Once verified, they can electronically submit their ballots, which the system automatically counts and securely archives in a database. This mechanism guarantees openness in result declaration, accelerates the voting process, and dramatically lowers human mistakes. Furthermore, fingerprint authentication is extremely accurate since every person has a different fingerprint, therefore almost impossible to fake or alter votes.

Among the many benefits of using a fingerprint voting system in departmental elections are improved security, environmental friendliness from lowered paper consumption, and cost-efficiency in terms of election management. By guaranteeing that voting is done honestly and without interference, it also helps voters to build trust. Strong encryption methods, safe database management, and backup authentication systems will, however, help to handle problems like system failures, data security hazards, and fingerprint identification mistakes. In total, a fingerprint-based voting system offers a contemporary, safe, and effective solution for departmental election running, hence guaranteeing fairness, accuracy, and simplicity of use for every participant.

.

2. PROSPECTIVE APPLICATION

Apart from internal elections, the fingerprint voting system offers improved security, effectiveness, and openness in many different voting and authentication scenarios. In college-wide elections, where student bodies, faculty, and administrative staff members can safely cast their ballots, one major use of is found.

This approach guarantees a just and trustworthy election process by removing the dangers of multiple voting and imposters.

Furthermore, corporate board elections could be run on fingerprint-based technology whereby executives and shareholders can vote on major decisions free from worry of illegal access or identity theft.

This system can also be used by governments for local and national elections to guarantee safe voting procedures and lower electoral fraud. Integrating it with e-governance systems enables remote electronic voting, which lets citizens to vote from several sites without jeopardizing the election's credibility. Furthermore, fingerprint verification can improve voting systems in community-based decision-making processes, cooperative societies, and non-governmental organizations (NGOs). Apart from elections, this approach can be used in attendance control to guarantee safe access to banned sites, businesses, and schools. In survey-based voting systems, where companies need reliable and secure participation in opinion polls or referendums, cryptography can also prove to be of value. Future uses could combine facial recognition and blockchain technology with developments in biometric technology to increase privacy and security even more. All in all, the fingerprint voting system might transform voting and authentication procedures in many sectors therefore guaranteeing accuracy, fairness, and efficiency in decision-making.

3. FINGERPRINT VOTING SYSTEM FOR DEPARTMENTAL ELECTIONS

A. Architecture

An easy-to-use platform where voters can view candidate lists and turn in their votes is created by the user interface (UI). Web-based or independent apps available via specified voting stations can support this UI. A vote is encrypted and sent to the backend system for safe processing and storage once it is cast. Vote integrity is guaranteed, several voting is stopped, and vote counting is automated by the backend processing mechanism. Result processing and real-time monitoring features are also part of this system. Encryption, blockchain integration, and access control mechanisms among other sophisticated security measures shield the system from cyber threats.

In departmental elections, this design guarantees equity and openness by offering a dependable, tamper-proof, and effective voting solution.

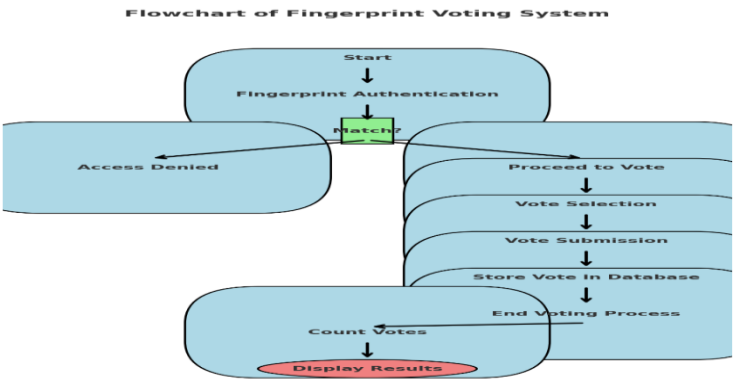

Figure 1: Flow of the Finger Print voting System

B. Level Of Description

Strategy Operating at several levels, the fingerprint-based voting system guarantees voting process efficiency, security, and correctness. Voters engage with the system at the consumer level via a user-friendly interface whereby they verify their identification using a fingerprint reader. Once validated, they may safely vote their chosen candidate and email their ballot.

The software checks voter fingerprints against a pre-registration database at the level of authenticity. By recognizing the biometric matches, the matching systems help to guarantee that only valid voters take part, so avoiding phony or repeated ballots. The system ensures honesty and stops tampering by encrypting votes securely in a database on the data processing level. Backend mechanisms manage votes in real-time, therefore limiting mistakes and need for manual interference. Security measures including encryption approaches, access control, and secure database management help to shield the system from unauthorized use and cyber threats.

4. CHALLENGES AND FUTURE SCOPE

A. Challenges

While the fingerprint voting system has advantages, several obstacles should be solved to guarantee accuracy and speed. Fingerprint recognition mistakes—one of the major obstacles—could be the result of sensor defects, spoiled or unclear fingerprints, or subpar fingerprint scans. Some old people or manual laborers with damaged fingerprints could in rare circumstances have problems verifying themselves.

Data security and privacy are also serious issues. Unauthorized access or hacking attempts could endanger voter information because fingerprint data is sensitive. To stop cyber one must unambiguously apply strong encryption solutions and safe database management.

Technical problems and failures of systems can also create hazards. Voting process disturbances caused by power outages, equipment malfunctions, or network breakdowns may call for contingency plans including spare verification means. Furthermore, the expense of implementation could be great—particularly in large-scale elections—since it calls for biometric scanners, secure servers, and trained staff for system maintenance.

At the level of the result computation, the system automatically tallies votes and produces results, therefore guaranteeing a fast, open, and just electoral process. This multilayered improves voting system trust and performance.

5. PARAMETERIZATION

To guarantee correctness, security, and efficiency, the fingerprint voting system depends on a number of important factors. The reliability of the system in confirming voter identities depends on the False Accept Rate (FAR) and False Rejection Rate (FRR), which serve to assess authentication accuracy. Fingerprint scanning time and vote submission response time control processing speed. To keep cyber attacks at bay, security parameters include database protection techniques and encryption standards. The system's scalability is based on the count of registered voters it can accommodate. User experience criteria stress interface accessibility and usability to help one to vote regularly.

Further more challenging is the acceptance and awareness among election officials as well as among voters. about the dependability of the system may call for awareness initiatives and training courses to help to establish trust and guarantee its flawless execution.

6. FUTURE SCOPES

Future developments of the fingerprint voting process could greatly increase electoral security and quality. One encouraging possibility is integration with facial recognition software, which offers a further level of verification to reduce identification mistakes.

One could use blockchain technology to improve security and openness, therefore guaranteeing unchangeable and verifiable votes. Furthermore, cloud-based remote voting would let voters have free online elections from anywhere without jeopardizing data integrity.

Further developments in AI-driven fraud detection and multi-bi difference authentication techniques will help to increase system accuracy. The fingerprint voting system could transform world elections with continuous developments so as to guarantee democracy in democratic procedures.

CONCLUSION

Election security is improved, voter fraud is stopped, and a clear and effective electoral process is guaranteed by the fingerprint voting system.

By means of biometric authentication, encryption, and automation, it eliminates duplication and human mistakes.

Future developments in multi-biometric verification, blockchain, and artificial intelligence will help its dependability, scalability, and worldwide acceptance in democratic systems even more.

ACKNOWLEDGEMENT

for their direction and support in this project, we genuinely grateful our technical support team together with our colleagues and mentors. the finished product of this study owes much to their valuable ideas and support.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING SUPPORT

The author declare that they have no funding support for this study.

REFERENCES

[1] Nigar, N. "A Proposed Framework for Fingerprint-based Voting." Journal of Information and Verification, vol. 2020.

[2] Agrawal, Shanu, Pradeep Majhi, and Vipin Yadav. "Fingerprint recognition based electronic voting machine." National Conference on Synergetic Trends in engineering and Technology (STET-2014). 2014.

[3] Gangadurai, E., R. Divakaran, and U. Aruneshwaran. "Fingerprint-Based Voting System." Journal of Telecommunication Study 8.2 (2023).

[4] Ashwini, K. "A Novel Multimodal Biometric Person Authentication System." PMC, vol. 2024.

[5] Sarfraz, M. "Introductory Chapter: On Fingerprint Recognition." IntechOpen, 2021.

[6] Agrawal, Shanu, Pradeep Majhi, and Vipin Yadav. "Fingerprint recognition based electronic voting machine." National Conference on Synergetic Trends in engineering and Technology (STET-2014). 2014.

[7] Olaniyi, Olayemi M., et al. "Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach." International Journal of Information Engineering and Electronic Business 8.5 (2016).[9] Ohio Revised Code "Chapter 1322 - Ohio Revised Code." 2025.

[8] Piratheepan, A., et al. "Fingerprint voting system using Arduino." Middle-East Journal of Scientific Research 25.8 (2017): 1793-1802.

[9] Kumar, D. Ashok, and T. Ummal Sariba Begum. "A novel design of electronic voting system using fingerprint." International Journal of Innovative Technology & Creative Engineering 1.1 (2011): 12-19.

[10] Ibrahim, Mohamed, et al. "Electionblock: An electronic voting system using blockchain and fingerprint authentication." 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C). IEEE, 2021.

[11] Hazzaa, Firas, and Seifedine Kadry. "New system of E-voting using fingerprint." International Journal of Emerging Technology and Advanced Engineering 2.10 (2012): 355-363.

[12] Gujanatti, Rudrappa B., et al. "A Finger Print based Voting System." International Journal of Engineering Research & Technology 4.5 (2015): 887-892.

[13] Vegesna, Vinod Varma, et al. "Finger Print Based Smart Voting System." Asian Journal of Applied Science and Technology 2.2 (2018): 357-361.

[14] Altun, Adem Alpaslan, and Metin Bilgin. "Web based secure e-voting system with fingerprint authentication." Scientific Research and Essays 6.12 (2011): 2494-2500.

[15] Nigar, Nahida, Mohan Lal Nath, and MD Toufiqul Islam. "A proposed framework for fingerprint-based voting system in Bangladesh." JOIV: International Journal on Informatics Visualization 4.1 (2020).

[16] Waili, Tuerxun, Amir NurIman Mohd Zaid, and Mohammed Hazim Alkawaz. "Advanced Voting System Using Fingerprint." International Journal on Perceptive and Cognitive Computing 6.2 (2020).

[17] Memon, K., Dileep Kumar, and S. Usman. "Next generation a secure e-voting system based on biometric fingerprint method." International Conference on Information and Intelligent Computing (IPCSIT). 2011.

[18] Hasta, Khadija, et al. "Fingerprint based secured voting." 2019 International Conference on Advances in Computing, Communication and Control (ICAC3). IEEE, 2019..